IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:	
Apple MacBook Pro, Serial No. C02SQ4IVGTFM, recovered from Room 534, Sheraton Station Square	MAGISTRATE NO. 19-346 **[UNDER SEAL]**
HP Laptop Model Lucasfilm Ltd., recovered from Room 534, Sheraton Station Square	MAGISTRATE NO. 19-347 **[UNDER SEAL]**
Apple iPhone 7, white front, red back, cracked screen, Model A1660, recovered from Cassio Orville Donald Slowden	MAGISTRATE NO. 19-348 **[UNDER SEAL]**
Black Apple iPhone, unknown model, recovered from Toyota Camry	MAGISTRATE NO. 19-349 **[UNDER SEAL]**
White Apple iPhone, unknown "S" model, recovered from Toyota Camry	MAGISTRATE NO. 19-350 **[UNDER SEAL]**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, David Anderchak, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of electronic devices that are currently in law enforcement possession, and the extraction from those devices of the electronically stored information described in Attachment B.

2. I have been employed as a Postal Inspector with the United States Postal Inspection Service since November of 2003. My duties include the investigation of crimes that involve the U.S. Postal Service and the U.S. mail. These crimes include mail fraud, mail theft, identity theft, burglaries and robberies of post offices, and counterfeit postal money orders. I am

currently assigned to the External Crimes Team within the Pittsburgh Office and I have served as a member of the Financial Crimes Task Force of Southwestern Pennsylvania. I am a "Federal Law Enforcement Officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. As a law enforcement officer, I have used a variety of methods to investigate crime, including, but not limited to, visual surveillance, witness interviews, the use of search warrants, confidential informants and undercover operations.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the devices in Attachment A contain evidence of violations of Title 18, Sections 1028 (identity fraud), 1028A (aggravated identity theft), 1029 (access device fraud), 1344 (bank fraud), 371 (conspiracy), or 1708 (theft of mail).

IDENTIFICATION OF DEVICES TO BE EXAMINED

5. Your affiant seeks a search warrant for the following electronic devices:

a. Apple MacBook Pro, Serial No. C02SQ4IVGTFM, recovered from Room 534, Sheraton Station Square

b. HP Laptop Model Lucasfilm Ltd., recovered from Room 534, Sheraton Station Square

c. Apple iPhone 7, white front, red back, cracked screen, Model A1660, recovered from Cassio Orville Donald Slowden

d. Black Apple iPhone, unknown model, recovered from Toyota Camry

e. White Apple iPhone, unknown "S" model, recovered from Toyota Camry

6. These devices have been in secure law enforcement custody since the times they were recovered (the circumstances of which are explained more fully below). In my training and experience, I know that the devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of law enforcement.

PROBABLE CAUSE

7. On Friday, February 7, 2019, your affiant was contacted by a Fraud Investigator from Citizens Bank. He reported that between January of 2018 to the present date of February 7, 2019, Citizens Bank, NA, a federally insured financial institution, has been experiencing an account takeover fraud. The fraud involved a caller contacting Citizens Bank's customer service contact center. The suspect would impersonate Citizens Bank customers and order replacement debit cards and debit card PIN reminders to the customers' addresses on file.

8. It was determined through the investigation that to facilitate the fraud, the suspect was fraudulently enrolling the Citizens Bank victim customers in the United States Postal Service's informed delivery service. This was done in order to receive notification of when the cards would be delivered, so they could be intercepted upon delivery by the United States Postal Service.

9. Once the cards were intercepted, the suspect(s) would use the debit cards to conduct ATM cash withdrawals in the victim customers' geographical area. In total, 104 victim customers have been targeted by this known fraud ring across the states of Massachusetts, Maine, Rhode Island, New Hampshire, Pennsylvania, and New York. The higher concentration of the fraud has occurred in the Pittsburgh, PA, Philadelphia, PA, and Massachusetts/Rhode

Island border area. To date, Citizens Bank has sustained a loss in the amount of $545,228 related to this fraud ring.

10. On February 7, 2019, Citizens Bank discovered that the suspect had ordered replacement debit cards and PIN reminders for four Citizens Bank customers located in McMurray, PA. The four customers are L.M. of 216 Robinhood Ln, J.L. 113 Maid Marion Ln, C.J. of 90 Will Scarlet, and E.H. of 233 King Richard Drive. All four replacement debit cards and PIN reminders were ordered through Citizens Bank's contact center on February 6, 2019.

11. On February 7, 2019, Citizens Bank Corporate Security Fraud Investigations notified United States Postal Inspector Dave Anderchak of the recently ordered replacement debit cards and PIN reminders and asked for the United States Postal Inspection Service's assistance in investigating the fraud.

12. The Citizens Bank Fraud Investigator informed your affiant that Citizens Bank replacement ATM cards and/or PIN numbers were mailed from Citizens Bank, 20 Cabot Road, Medford, MA 02155 and were due for delivery on Monday, February 11, 2019.

13. On the morning of February 11, 2019, your affiant confirmed with USPS management that the following four Citizens Bank mailings had arrived and were due for delivery later in the afternoon of February 11, 2019:

E.H.
233 King Richard Drive
McMurray, PA 15317

C.J.
90 Will Scarlet Road
McMurray, PA 15317

J.L.
113 Maid Marion Lane
McMurray, PA 15317

J.L.
113 Maid Marion Lane
McMurray, PA 15317

14. On Monday February 11, 2019, Postal Inspectors along with officers from the Peters Township Police and the Department of Homeland Security initiated surveillance in the McMurray, PA neighborhood that included 113 Maid Marion Lane, McMurray, PA 15317, 90 Will Scarlet Drive, McMurray, PA 15317, and 233 King Richard Drive, McMurray, PA 15317.

15. At approximately 2:05 pm, U.S. Mail was delivered to the 90 Will Scarlet Drive address. At approximately 2:08 pm, Postal Inspector James Ali observed an African-American male operating a white four door sedan bearing an out of state license plate stop in front of the 90 Will Scarlet Drive address. The vehicle stopped at the mailbox and the male accessed the mailbox for 90 Will Scarlet Drive before driving from the area.

16. Inspector Ali checked the mailbox and confirmed that mail was present, but not the Citizens Bank mailings.

17. Moments later Postal Inspector Brian Plants who was conducting surveillance at 233 King Richard Drive, McMurray, PA observed the same four door white sedan drive slowly past the 233 King Richard Drive address.

18. At approximately 2:10 pm, your affiant along with Peters Township Sergeant Rob Kemp observed a white four door Toyota Camry bearing Connecticut license plate AN06784 driven by an African-American male in the 200 block of King Richard Drive.

19. Your affiant and Sergeant Kemp initiated a traffic stop of the vehicle and identified the driver of the vehicle by license as:

Cassio Orville Donald Slowden
8203 S. Palm Drive, Apt. 517
Pembroke Pines, FL 33025

20. As Slowden exited the vehicle, officers noticed an opened Citizens bank mailing in the name of C.J., 90 Will Scarlet Drive, McMurray, PA 15317 in the bottom side compartment of the driver's side door of the vehicle.

21. Your affiant and officer Kemp secured Slowden and conducted a brief search for officer safety. At this time, officers discovered a room key holder for Room 534, a Sheraton room key, and a meal coupon for the Sheraton at Station Square, 300 West Station Square Drive, Pittsburgh, PA 15219, with a departure date of February 15, 2019.

22. Also found on the person of Slowden was an Apple iPhone 7, white front, red back, cracked screen, Model A1660.

23. Slowden was arrested on state charges.

24. On February 11, 2019, your affiant applied for and received federal search warrants for Room 534 of the Sheraton at Station Square and the white Toyota Camry described above, at Mag. Nos. 19-287 and 19-288 (under seal).

25. Additionally, a criminal complaint was filed, and an arrest warrant was issued, for Slowden at Mag. No. 19-289 (under seal).

26. On the evening of February 11, 2019, law enforcement executed the search warrant on Room 534 of the Sheraton at Station Square. Investigators discovered stolen U.S. mail from a second neighborhood in the Pittsburgh area. Investigators also located an Apple MacBook Pro, Serial No. C02SQ4IVGTFM, and an HP Laptop model Lucasfilm Ltd.

27. The same night, law enforcement executed the search warrant on the white Toyota Camry. In the vehicle, investigators discovered U.S. Mail stolen from the 90 Will Scarlet address noted above, as well as a black Apple iPhone, unknown model, and a white Apple iPhone, unknown "S" model.

28. Your affiant believes that the information contained within the devices may help to identify the other suspects and conspirators, instructions to others regarding the crimes, as well as other communications made in furtherance of the conspiracy, including contacts made to financial institutions.

29. Without turning on the cellular phones, and searching them, it is not possible to tell what telephone number is associated with the phones. With the authorization sought in this search warrant, your affiant will be able to identify the associated telephone numbers. A subpoena to the cellphone provider for this telephone number can then be completed to obtain additional details about the account holder, including associated addresses, telephone numbers and methods of payment.

30. Your affiant also knows that the devices are capable of not only voice communications, but also text messaging, SMS chat messaging, and email communications. Your affiant also knows that these devices may also have significant electronic storage capability, as well as internet browsing and computer functions, and memory storage which may reveal additional evidence of the crimes.

31. Your affiant also knows through training and experience, that the conspirators of financial crimes and identity theft crimes communicate by electronic means. And, that electronic devices such as computers, tablets, cell phones or other electronic storage devices are used to store debit/credit card account information and identification documents since these devices can store thousands of pieces of data including contacts with financial institutions and information from financial institutions.

32. Therefore, your affiant has reason to believe that the electronic devices described above contain evidence concerning the offenses of mail theft, bank fraud, identity fraud, aggravated identity theft, access device fraud, and conspiracy.

33. The devices will be provided to the computer forensic examiners at the United States Secret Service for examination.

34. The devices are currently in storage at the offices of the United States Secret Service at 112 Washington Place, 2 Chatham Center, Suite 1610, Pittsburgh, PA 15219. In my training and experience, I know that the devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession law of enforcement.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

35. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

Forensic Evidence: Deleted Files, User Attribution

36. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory

paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

37. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

38. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

39. I submit that this Affidavit supports probable cause for a search warrant authorizing the search of the devices described in Attachment A, to seek the items described in Attachment B.

40. Based on my training and experience, and the facts set forth in this Affidavit, there is probable cause to believe that there is evidence of violations of the federal crimes of mail theft, bank fraud, identity fraud, aggravated identity theft, access device fraud, and conspiracy contained within the electronic devices.

The above is true and correct to the best of my knowledge.

Respectfully submitted,

David Anderchak
U. S. Postal Inspector
U.S. Postal Inspection Service

Subscribed and sworn to before me
on February 19, 2019:

HONORABLE CYNTHIA R. EDDY
CHIEF UNITED STATES MAGISTRATE JUDGE